

GE Vernova Electrification Software SWMFS Improper Authentication Vulnerability

Vulnerability ID: CVE-2025-3222
CVSS v4.0 Score: 9.3
CVSS Severity: Critical
CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Overview

GE Vernova's Electrification Software business (GE Vernova) has become aware of a vulnerability that has the potential to affect the authentication mechanism (Vulnerability) in its Smallworld Master File Server (SWMFS) Software (Affected Software) affecting Smallworld Deployments from v3.0.0 up to v5.3.3 (for Linux deployments) and v5.3.4 (for Windows deployments), which could lead to unintended behavior.

After assessing the Vulnerabilities for the Affected Software, GE Vernova determined that the Vulnerability could be exploited to circumvent authentication and possibly perform elevated commands.

Exploit of the Vulnerability is only possible by a user with knowledge of the system, the underlying protocol, and the rights associated to users with already provisioned access. Secure deployment and strong access management for users is essential. GE Vernova strongly recommends that customers adhere to the most recent Secure Deployment Guide (SDG) instructions – [Smallworld Documentation](#).

GE Vernova has resolved the issue in Smallworld v5.3.4 for Linux SWMFS users and v5.3.5 for Windows SWMFS users.

Due to the many stringent requirements for Operational Technology (OT) and Industrial Control Systems (ICS), GE Vernova strongly recommends current users to consider their defense-in-depth strategies, including network segmentation, to understand the true risk of this exposure in their environment. An open-source model has been developed to assist in this process and can be found here: [Industrial Vulnerability Scoring System \(IVSS\)](#).

Affected Software

Affected

Any Smallworld deployment (SW) not using Desktop authentication via an authentication server, such as UAA or Zitadel, and not following the secure deployment guidelines. This was available from SW5.3.4 for deployments using Linux to run SWMFS and from SW5.3.5 for deployments using Windows to run SWMFS. Hence, any products from SW3.0.0 to SW5.3.3 would have no way of being configured to remove the CVE.

Not Affected

- Any Smallworld deployment using Desktop authentication via an authentication server and following the Secure Deployment Guidelines.

Solution

GE Vernova recommends that users upgrade to the appropriate non-affected version listed above in accordance with their use case and architecture as this is the most complete method to address the Vulnerability.

Also, users are strongly advised to follow the SDG instructions. The complete SDG can be found in the [Smallworld Documentation](#).

To obtain the latest version of SWMFS, please contact your local support representative at [Customer Center](#).

GE Vernova thanks Théo GOBINET and Azaël MARTIN of ENGIE IT Offensive Cybersecurity Team for bringing information about the Vulnerability to its attention.

Disclaimers

This advisory (Advisory) is subject to the terms and conditions contained in your underlying license agreements or other applicable agreements with GE Vernova. Due to ongoing product enhancements, GE VERNOVA reserves the right to change or update its advisories (including this Advisory) without advance notification to you. GE VERNOVA DIGITAL DISCLAIMS ANY REPRESENTATION OR WARRANTY THAT ITS PRODUCTS, SERVICES OR SOLUTIONS WILL OPERATE FREE FROM ERROR, INTERRUPTION, OR DISRUPTION, INCLUDING, WITHOUT LIMITATION, DUE TO CYBER-ATTACKS, MALICIOUS OR OTHERWISE, OR THAT ANY PRODUCTS, SERVICES OR SOLUTION PROVIDED BY GE VERNOVA WILL PROVIDE COMPLETE OR COMPREHENSIVE

PROTECTION AGAINST ALL POSSIBLE SECURITY VULNERABILITIES OR UNAUTHORIZED INTRUSIONS, INCLUDING THE VULNERABILITY.

Auto-Notification

Please visit the customer profile page on the support site to sign up for auto-notifications for GE Vernova Software products to receive immediate notice of security alerts and information.

Instructions can be found here; [How to sign up for Auto-Notifications](#).

Change Log

Date	Change(s)
10/7/2025	Initial version
11/3/2025	Updated for public release